DATA MANAGEMENT au LAPP

N. NEYROUD, D. SANCHEZ, I. MIEVRE, E. FEDE

DATA Project management (NN): Bilan 2016

1) Mise en place de réunions régulières:
   - DATA Executive Board meetings tous les deux mois
   - Data global meetings tous les 15-30 jours, meetings spécialisés
2) Coordination de la mise à jour du TDR en Mars 2016
3) Décision fin 2015 de réorganiser la partie logiciel de CTA (reshuffle)
   - Suite à la proposition de méthodologie faite par DATA lors du Consortium meeting de Kashiwa en mai 2016
   - => Plus de 6 réunions “Architecture Workshop” avec le Project Office pour définir l’Architecture de tout le logiciel CTA et redistribuer les responsabilités (Actuels DATA/ACTL)
4) Software Development Plan & Standards – Basé sur le travail d’animation fait par le LAPP il y a deux ans (CB, NN)
5) Support aux outils redmine/SVN/Jenkins largement utilizes par CTA (CB)

DATA Management : Perspective 2017

Selon le retour du travail sur l'Architecture prévu fin janvier 2017:

- réattribution des responsabilités

IC Infrastructure (NN): Bilan 2016

1) Equipe Authentication & Authorization (NN, DS, Italy, Polish, Observatoire de Meudon)
   - Animation de l'équipe
   - Use Case, User Requirements, tableau de comparaison des deux prototypes actuels: Catania & CYFRONET
2) Implication du LAPP dans les simulations CTA sur la grille (EF,CB)
3) Projet HSNSciCloud de Cloud privé – public (NN, EF, LUPM) en cours): Use Case CTA
4) Réponse à l'appel d'offre "Science Data Management Center" (GL + NN)
5) Proposition de Consortium entre 3 datacenters CCIN2P3, PIC Barcelona, INFN Bologna (CODAC) dans la réponse EOI (Expression Of Interest) du LAPP (GL + NN)

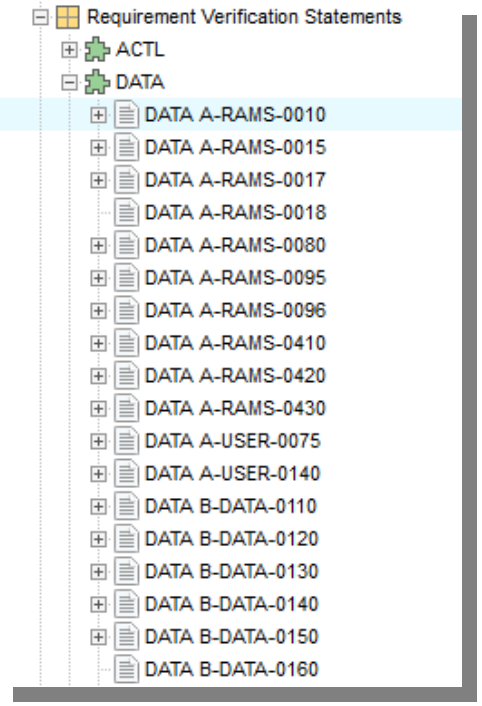
IC Infrastructure: Perspective 2017

1) Mise à jour des coûts IC Infrastructure (NN, EF) - en cours
2) Sélection d'un système A&A – en lien également avec le projet ASTERICS
3) Rédaction d'une première version de MoU CODAC en concertation avec les 3 (4?) datacenters
4) Gateway: Selon la redistribution des responsabilités
5) CTADIRAC (LUPM) en constante amélioration – lien avec le Cloud, amelioration des performances
6) En attente du call de l'Observatoire pour la partie Computing Model.

Qualité (IM): Bilan 2016

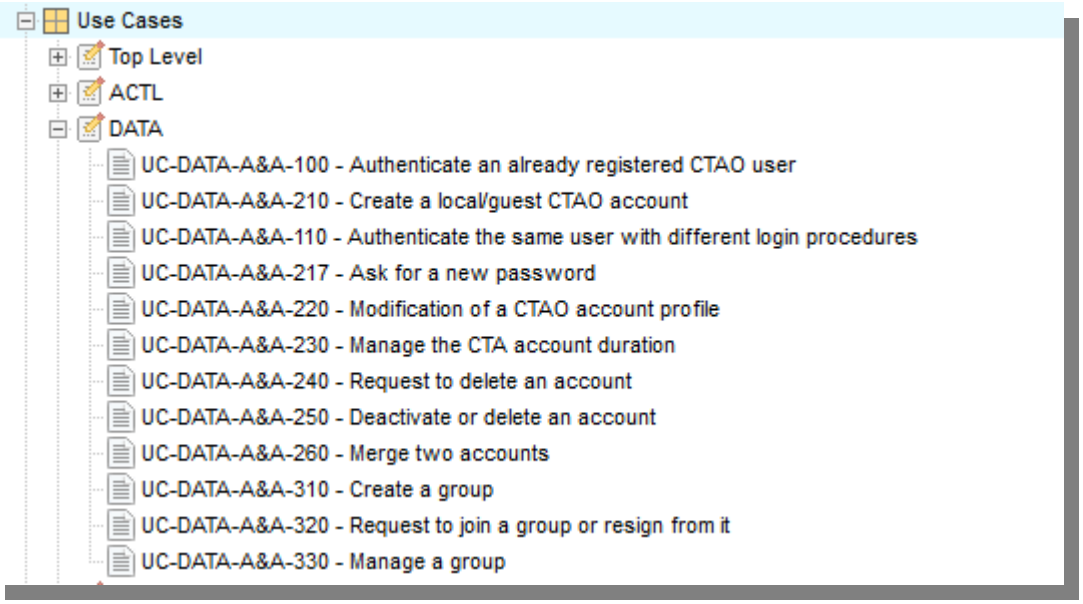
- Mise à jour de la partie plannings du TDR (mars 2016)
  - Jalons Externes
  - Plannings DATA Management

- JAMA RVS :
  - Mise en adéquation des Requirement Verification Status de JAMA avec le document « DATA Preliminary Design Verification Document »



Bilan 2016

- JAMA Use Cases :
  - Création en séances de Use Cases de la partie Authentication & Authorization



Perspectives 2017

- Mise à jour de la partie plannings du TDR
  - Jalons Externes
  - Plannings DATA Management

- JAMA :
  - RVS : mise à jour et corrections
  - Use Cases : continuation des UC A&A et des autres UC

- Rédaction du « Software Development Plan and Standards » for DATA Management (divisé en 3 documents).

Authentication & Authorization

Authentication
is the process of identifying an individual using the credentials of that individual.

Authorization is the process of determining whether an authenticated individual is allowed to access a resourceor perform a task

Role-Based Authorization
When a user or group is added to a role, the user or group automatically inherits the various security permissions

From A. COSTA (Bologna)

A&A : use cases

List of existing or identified A & A use cases

Use Case	Description	External/Internal system	ID
Authenticate an already registered CTAO user	User executes a login procedure to access his CTAO account environment using his specific local/guest A&A login/password. (Issue nb: https://forge.in2p3.fr/issues/13965)	Gateway/A&A	UC-DATA-A&A-000100
Authorize a user based on his institute/laboratory account	User presents either his X509 certificate or login/password issued by his organization/institute to access his CTAO account environment in CTAO Science Gateway. Same functionality from a DATA Application not integrated in the Gateway. (Issue nb: https://forge.in2p3.fr/issues/13968)	Gateway/DATA Applications/A&A	UC-DATA-A&A-000120
Create a local/guest CTAO account	User could request a local/guest A&A login/password to access his CTAO Science Gateway personal environment. A Captcha mechanism and email of confirmation should be planned for security. This created CTAO account, created automatically with no CTAO approval, will have limited privileges. (issue nb: https://forge.in2p3.fr/issues/13969)	Gateway/A&A	UC-DATA-A&A-000210
Multiple affiliation accounts	It must be possible to allow that same user can alternatively use different authenticated methods and could be recognized by the system as the same CTAO account owner. (Issue nb: https://forge.in2p3.fr/issues/13970)	Gateway/DATA Applications/A&A	UC-DATA-A&A-000215

A&A : use cases

List of existing or identified A & A use cases

Use Case	Description	External/Internal system	ID
Authenticate an already registered CTAO user	User executes a login procedure to access his CTAO account environment using his specific local/guest A&A login/password. (Issue nb: https://forge.in2p3.fr/issues/13965)	Gateway/A&A	UC-DATA-A&A-000100
Authorize a user based on his institute/laboratory account	User presents either his X509 certificate or login/password issued by his organization/institute to access his CTAO account environment in CTAO Science Gateway. Same functionality from a DATA Application not integrated in the Gateway. (Issue nb: https://forge.in2p3.fr/issues/13968)	Gateway/DATA Applications/A&A	UC-DATA-A&A-000120
Create a local/guest CTAO account	User could request a local/guest A&A login/password to access his CTAO Science Gateway personal environment. A Captcha mechanism and email of confirmation should be planned for security. This created CTAO account, created automatically with no CTAO approval, will have limited privileges. (issue nb: https://forge.in2p3.fr/issues/13969)	Gateway/A&A	UC-DATA-A&A-000210
Multiple affiliation accounts	It must be possible to allow that same user can alternatively use different authenticated methods and could be recognized by the system as the same CTAO account owner. (Issue nb: https://forge.in2p3.fr/issues/13970)	Gateway/DATA Applications/A&A	UC-DATA-A&A-000215

STILL A LOT OF WORK : JAMA

A&A : Compte et Groupe

*A **CTAO account** is any user account registered in the A&A system with a unique "AccountId" **(Persistent Id)**.*

Notion de Groupe

- *A Group is understand as a list of Users. The group is associated with a list of roles. A group owner is able to invite/remove users in the group. He can also add roles from the associated list of roles to a specific member.*

→ Ex : auteurs d'une proposition d'observations

Accounts

Theres is 3 types of account

- CTA member - LDAP
- Federation user – edugain
- Local account – CTAO account

CTAO account has minimal right and can be created by anyone

- The A&A system will have the standard option (request lost password, account creation, etc…)
- Already identified user must be able to request change part of his CTAO account profile
- A user can ask to delete his account.
- The A&A administrator can deactivate or delete any account.
- The A&A administrator is able to merge two accounts

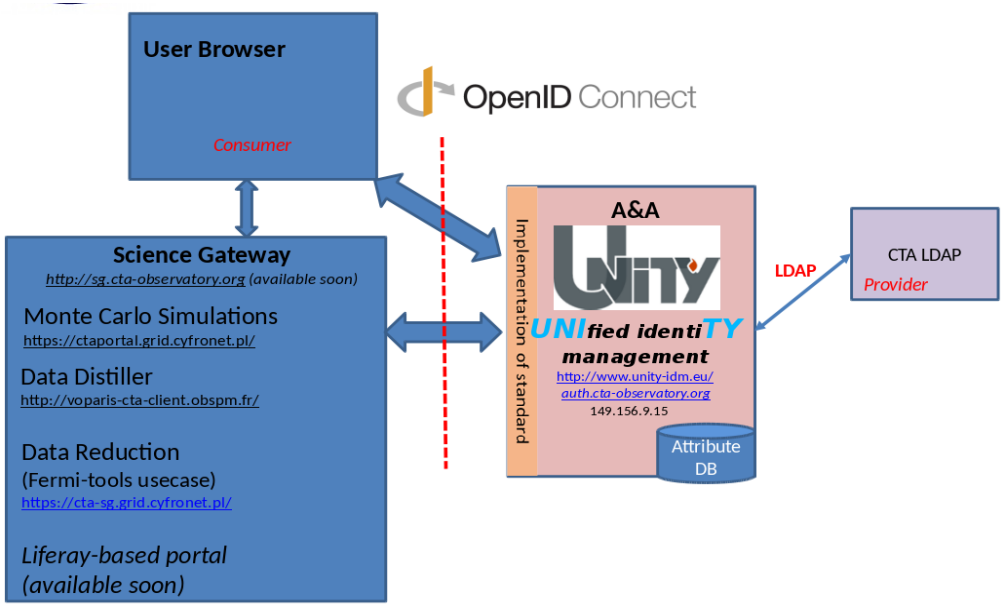
USER Requirements

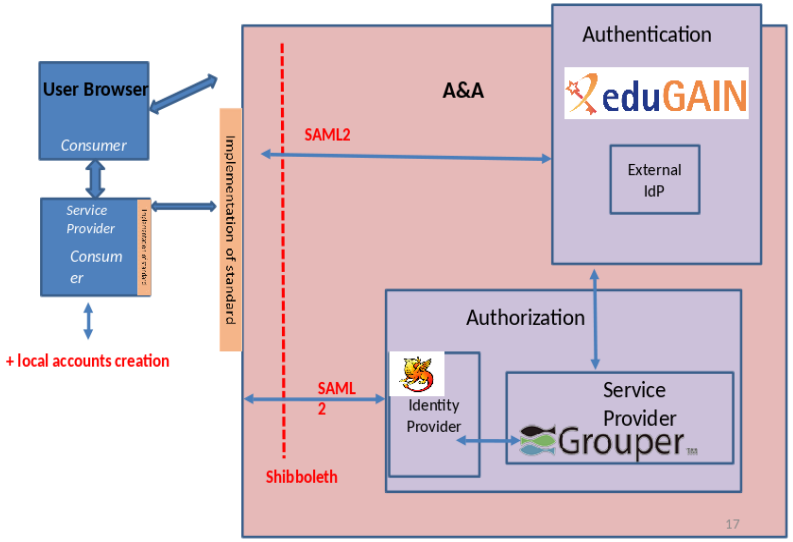
https://forge.in2p3.fr/projects/a-a/wiki/A_and_A_User_Requirements

User Requirements are grouped in the following Classes:

- Authentication capabilities
- Authorization capabilities
- Account Management capabilities
- Group Management by users/group owner
- Interfaces
- Availability
- Performance
- Security
- Portability

A&A : Prototypes





Unity (Pologne)

Shibboleth+Grouper (INAF)

Sélection d'un prototype par le PO